CLAIMS

Having thus described our invention, what we claim as new and desire to secure by Letters Patent is as follows:

1. A method of guaranteeing authenticity of an object, comprising:

providing a sample of material obtainable only by at least one of chemical and physical processes such that the sample is random and not reproducible;

associating a number reproducibly to any said sample by using a specific reader; and

forming at least one coded version of said number, said at least one coded version being obtained by a key signature, and said coded version being recorded into an area of said object.

2. The method according to claim 1, wherein said object includes a chip having a recording support positioned on said object, said method further comprising:

when the number associated to said sample is only essentially reproducible, recording said number on said object, either on the chip or on said recording support for said chip.

3. The method according to claim 1, wherein said object comprises a smart card.

4. The method according to claim 3, wherein said smart card incorporates a chip.

5. The method according to claim 1, wherein said associating comprises:

reading the sample exactly by the reader;

sending a result of the reader to a processor, which associates with the reading of the sample said number;

sending said number to a second processor containing a secure hash function, details of which are made public, and a secret part of said key signature, said key signature comprising a public key signature, wherein said second processor computes a coded version of the hash of said number appended with a predetermined, optional data; and

outputting said coded version to said object.

6. The method according to claim 5, wherein upon introducing the object into a second reader, said second reader extracts said number and said coded version using a public part of the public key signature scheme, such that if the information of said number and said coded version are compatible, the object is deemed authentic.

7. The method according to claim 1, wherein said key signature includes using public key cryptography.

8. The method according to claim 1, further comprising:

reading, by a reader, the sample in an imprecise manner such that sequential readings are not exactly the same,

wherein said object carries a chip and a recording of a digital representation of the sample from the reader of a subject associated with the object.

9. The method according to claim 8, further comprising:

sending a result of the reader to a processor, which associates with the reading of the sample said number;

sending said number to a second processor containing a secure hash function, details of which are made public, and a secret part of said key signature, said key signature comprising a public key signature, wherein said second processor computes a coded version of the hash of said number appended with a predetermined, optional data; and

outputting said coded version to said chip.

10. The method according to claim 9, wherein upon introducing the object into a second reader, a different reading of said sample occurs such that

the first reader reads the sample to deliver *R(S)* and the second reader reads the sample to deliver *R0(S0)*, said method further comprising:

determining by a comparator whether the readings by said first and second readers are less than or equal to a predetermined threshold to accept the object, at least temporarily, as authentic.

11. The method according to claim 10, further comprising:

reading said coded version by said chip and verifying said coded version against said number by using a public part of the public key signature; and

if said number and said coded version read by said chip are compatible, accepting the card as authentic.

12. The method according to claim 8, further comprising:

delivering by said reader an actual reading *R(S)* and delivering by a second reader an original reading as *R0(S0)*;

processing said readings by first and second processors to deliver *N(R(S)* and *N(R0(S0))*, respectively; and

determining by a comparator whether outputs from said first and second processors have a value no more than a predetermined threshold, to temporarily accept the object as authentic.

13. The method according to claim 12, further comprising:

reading the coded version in said chip and verifying said coded version against said number by using a public portion of a public key signature; and if the information in said number and that read in said chip are compatible, accepting said object as authentic.

14. The method according to claim 1, further comprising:

sensing a degeneration of said sample.

15. The method according to claim 14, wherein said sensing includes comparing a difference between an actual reading vector and an original reading vector against a threshold;

forwarding a result of the reader to a processor, which associates with the reading of said sample a transformed vector $K(N0(R0(S0)))$, where K is a transformation matrix; and

forwarding the transformed vector to a second processor including a secure hash function, details of which are made public, and a secret part of a public key signature scheme.

16. The method according to claim 15, wherein said object includes a chip, and wherein said second processor computes a coded version of the hash function of the transformed vector appended with predetermined optional

external data, to provide a coded number, said coded number being put on said chip,

wherein upon introducing the card to a second reader, a predetermined different reading of the sample is performed.

17. The method according to claim 16, wherein an actual reading made by a first reader is transformed into a transformed vector *KN*, and wherein an original transformed vector *KN0* is delivered by a second reader, and

wherein the transformed vector, *KN* is compared against the original transformed vector *KN0* by a comparator such that if the two transformed vectors have a value within a predetermined closeness, the object is temporarily accepted as authentic.

18. The method according to claim 17, further comprising:

reading by said chip the coded version and verifying said coded version again the transformed vector using a public part of the public key signature; and

accepting the object as authentic if the transformed vector and the coded version read in said chip are compatible.

19. The method according to claim 1, wherein said object being authenticated comprises a piece of paper.

20. The method according to claim 1, wherein a sequence of data associated with said sample, said sample, and certificates associated with said sample and said data are precomputed.

21. The method according to claim 20, wherein new data and its certificate are computed dynamically.

22. The method according to claim 1, wherein said key signature includes using private key cryptography.

23. The method according to claim 1, wherein said specific reader captures information out of the sample by one of a scanning and globally.

24. The method according to claim 1, wherein said sample includes at least one of a mineral and a glass, selectively covered by a carbon film and affixed to said object.

25. The method according to claim 1, wherein said coded version of said number includes at least one of optional data appended to said number and a hash of said number with said optional data.

26. The method according to claim 1, wherein data linked to the sample of material is selectively changeable.

27. The method according to claim 1, wherein said sample of material is selectively changeable over time.

28. The method according to claim 1, wherein said data is selectively changeable when said sample is changed.

29. The method according to claim 20, wherein said data is selectively changeable when said sample is changed.

30. The method according to claim 1, wherein new data associated with said sample and its certificate are computed dynamically.

31. The method according to claim 1, wherein at a time of creation of said object, said coded version of said number is stored in memory for later comparison when said object is presented for authentication.

32. The method according to claim 1, wherein a plurality of coded versions of numbers are recorded into said object.

33. A method of preventing cloning of an object, comprising:

providing a sample of material obtainable only by at least one of chemical and physical processes such that the sample is random and not reproducible;

associating a number reproducibly to any said sample by using a specific reader; and

forming at least one coded version of said number, said at least one coded version being obtained by a public key signature, and said version being recorded into an area of said object.

34. A method of preventing imitation of a smart card, comprising:

providing a sample of material obtainable only by at least one of chemical and physical processes such that the sample is random and not reproducible;

associating a number reproducibly to any said sample by using a specific reader; and

forming at least one coded version of said number, said at least one coded version being obtained by a public key signature, and said version being recorded into an area of said object.

35. A system for guaranteeing authenticity of an object, comprising:

a sample of material obtainable only by at least one of chemical and physical processes such that the sample is random and not reproducible, said sample being placed on said object;

means for associating a number reproducibly to any said sample by using a specific reader; and

means for forming at least one coded version of said number, said at least one coded version being obtained by a public key signature, and said version being recorded into an area of said object.

36. A signal-bearing medium tangibly embodying a program of machine-readable instructions executable by a digital processing apparatus to perform a method for computer-implemented guaranteeing of authenticity, said method comprising:

providing a sample of material obtainable only by at least one of chemical and physical processes such that the sample is random and not reproducible;

associating a number reproducibly to any said sample by using a specific reader; and

forming at least one coded version of said number, said at least one coded version being obtained by a key signature, and said version being recorded into an area of said object.